

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



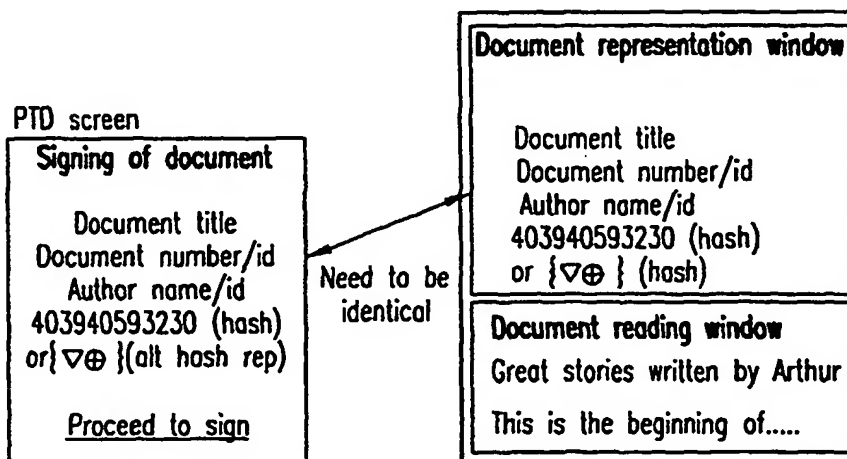
(43) International Publication Date
13 December 2001 (13.12.2001)

PCT

(10) International Publication Number
WO 01/95071 A2

- (51) International Patent Classification⁷: **G06F 1/00** (74) Agent: **ERICSSON MOBILE COMMUNICATIONS AB**; IPR Department, S-221 83 Lund (SE).
- (21) International Application Number: **PCT/EP01/06349**
- (22) International Filing Date: **5 June 2001 (05.06.2001)**
- (25) Filing Language: **English**
- (26) Publication Language: **English**
- (30) Priority Data:
60/209,504 5 June 2000 (05.06.2000) US
60/249,819 17 November 2000 (17.11.2000) US
09/803,210 8 March 2001 (08.03.2001) US
- (71) Applicant (for all designated States except US): **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-126 25 Stockholm (SE).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **SKUBIC, Janez** [SI/SE]; Radisvägen 46, S-165 73 Hässelby (SE). **DENT, Paul** [GB/US]; 637 Eaglepoint Road, Pittsboro, NC 27312 (US). **SMEETS, Bernard** [NL/SE]; Dalbackavägen 11, S-240 10 Dalby (SE). **ANDERSSON, Stefan** [SE/SE]; Koltrastgränd 23, S-230 41 Klågerup (SE). **LINDSKOG, Helena** [SE/SE]; Tomtebogatan 6, S-654 63 Karlstad (SE). **NILSSON, Mikael** [SE/SE]; Hagagatan 14B, S-652 20 Karlstad (SE).
- (81) Designated States (national): AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- Published:**
— without international search report and to be republished upon receipt of that report
- For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: **METHOD FOR SIGNING DOCUMENTS USING A PC AND A PERSONAL TERMINAL DEVICE**



(57) Abstract: A system and method for digitally signing a document including a personal computer which receives the document to be digitally signed. A representation of the document is created from the document and this representation is forwarded to a personal trusted device such as a mobile terminal, personal computer, etc. The user may then view the document on the personal computer and provide a digital signature of the document from the personal trusted device.

WO 01/95071 A2

METHOD FOR SIGNING DOCUMENTS USING A PC AND A PERSONAL TERMINAL DEVICE

TECHNICAL FIELD

The present invention relates to the digital signing of documents, and
5 more particular, to the digital signing of documents using a personal
terminal device.

BACKGROUND OF THE INVENTION

The WAP/WIN protocols enable personal trusted devices, such as
10 mobile telephones, laptop computers, and personal data assistants, to
become powerful signature generation devices that can be used to sign
data from any PC, website, etc. Currently, there is only one way of
performing digital signatures using a PTD such as a mobile terminal.
This method involves the use of the WML-Script function signTEXT. The
15 signTEXT function takes text as input and displays it to the user so
that the user may generate a signature. The trust model is very simple
and puts the responsibility on the user to confirm that what you see is
what you sign. This is also referred to as the WYSIWYS principle.

The major problem with current systems using PTDs for digitally
20 signing documents is the WYSIWYS principle. The problem arises because
of the limited display capabilities of a PTD. It is generally not
possible to display large documents on a PTD device such as a mobile
terminal. Additionally, the buffering and content parsing capabilities
of a mobile terminal are very limited and may not contain the proper
25 applications to display the document in its received format. For
example, if a Word document is received, the PTD must have the ability
to display Word format.

Thus, the user is not actually digitally signing the entire
document but only a small representation of the entire document referred
30 to as a hash. This violates the WYSIWYS trust model, and a user can no
longer verify that what he signs is necessarily what he thinks he
signs. Thus, an improved method for enabling the use of PTD devices

such as mobile terminal for digitally signing documents while still enabling a user to view all of the necessary portions of a document being signed is needed.

5 **SUMMARY OF THE INVENTION**

 The present invention overcomes the foregoing and other problems with a method for digitally signing a document using a PTD that also provides a user the opportunity to view the document substantially in its entirety. The document to be digitally signed is received at a
10 first location where the document may also potentially be displayed. A representation of the document is generated at the first location and the representation of the document is forwarded to a personal trusted device (PTD). At the personal trusted device the user may digitally sign the representation of the document after viewing the complete
15 document at the first location.

BRIEF DESCRIPTION OF THE DRAWINGS

 A more complete understanding of the method and apparatus of the present invention may be obtained by reference to the following Detailed
20 Description when taken in conjunction with the accompanying Drawings wherein:

 FIGURE 1 is a block diagram illustrating the relationship between a document and a hash of a document;

 FIGURE 2 illustrates the use of a mobile terminal for digitally
25 signing a document in conjunction with a viewing location;

 FIGURE 3 illustrates a first embodiment wherein the digital signature is provided using the combination of a trusted PC and a mobile terminal;

 FIGURE 4 is a flow diagram illustrating the method of FIGURE 3;

30 FIGURE 5 is an illustration of alternative embodiment wherein a digital signature is obtained using a crypto module and a mobile

terminal;

FIGURE 6 illustrates the document and hash displays at a PC and a mobile terminal;

FIGURE 7 is a flow diagram illustrating the method of FIGURE 5;

5 FIGURE 8 illustrates a method for obtaining a digital signature between a PC, a trusted party and a mobile terminal;

FIGURE 9 is a flow diagram illustrating the method of FIGURE 8;

FIGURE 10 illustrates the use of streaming data between a PC and a mobile terminal to obtain a digital signature;

10 FIGURE 11 is a flow diagram illustrating a first method of utilizing streaming data as illustrated in FIGURE 10;

FIGURE 12 illustrates a second method for utilizing streaming data as shown in FIGURE 10.

15 FIGURE 13 is a block diagram of a further embodiment including a customer PC, merchant server and customer mobile terminal and the interactions therebetween; and

FIGURE 14 is a flow diagram illustrating the method of the system illustrated in Figure 13.

DETAILED DESCRIPTION

Referring now to the drawings, and more particularly to the FIGURE 1, there is illustrated a document 10 and a hash 15 of the document 10. The document 10 would consist of a copy of text which may comprise a contract, letter, sales receipt, email or any other item that may need to be signed by a user. The hash 15 contains a listing of information pertaining to the document. This information could include, for example, a document title, a document number/id, an author/name id, and a hash representation which may be numeric, alpha-numeric or symbolic.

Referring now to FIGURE 2, there is illustrated a general representation of the manner for using a personal trusted device such as a mobile terminal 20 to digitally sign a document 10. Alternatively, the personal trusted device could be a laptop computer, personal data assistant, pager or another mobile electronic device. The document 10 is forwarded to some type of viewing location 25 such as a PC, trusted server or other area which will be discussed momentarily. The document 10 is provided to the viewing location 25, where it may be displayed in its entirety by a user wishing to digitally sign the document 10. The hash 15 is created at the viewing location 25 or at a location associated with the viewing location 25 such that the hash 15 may be transmitted to the mobile terminal 20 over a wireless or wireline connection. The user may view the document 10 in its entirety at the viewing location 25 and digitally sign the hash 15 at the mobile terminal 20.

A first embodiment is illustrated in FIGURE 3 where there is illustrated a method for obtaining a digital signature using a trusted PC 30. In this embodiment, the information contained on the trusted PC 30 is assumed to be accurate, including the document 10, and the only thing needed to be protected is the communications channel 32 between the trusted PC 30 and the mobile terminal 20. The communications channel 32 may utilize a serial cable, infrared link or Bluetooth

(Bluetooth is a trademark of Telefonaktiebolaget LM Ericsson) pairing for transmitting data. The only requirement for this embodiment is that the trusted PC 30 be authenticated and the integrity of the data be protected over the communications link 32.

5 Referring now to FIGURE 4, the trusted PC 30 receives the document 10 to be digitally signed at step 35. The mobile terminal 20 must authenticate the trusted PC 30 at step 40 to confirm that the mobile terminal 20 is linking with the proper trusted PC 30. After authentication, the communications channel 32 is established at step 45,
10 and the hash 15 of document 10 is transmitted at step 50 to the mobile terminal 20. The user views the entire document 10 at the trusted PC 30 and provides the digital signature at step 55 using the mobile terminal 20. The digital signature may be automatically provided by entering a PIN number at the mobile terminal 20.

15 A further embodiment, shown in FIGURE 5, uses a crypto module 70 which may be implemented in a browser 65 contained within a PC 60. The crypto module 70 is integrated within the browser 65 and implements cryptography such as PKCS#11 and MS CAPI. In order to integrate the crypto module 70 within the browser 65, authenticity and integrity of
20 the crypto module 70 must be verified by the PC operating system or the browser 65 before the module 70 is used. The crypto module 70 displays the document 10 to be signed along with the hash 15 to be transmitted to the mobile terminal 20 as is illustrated in FIGURE 6. The mobile terminal 20 may also authenticate and integrity protect the
25 communications channel 75 between the PC 60 and mobile terminal 20 as discussed previously with respect to FIGURES 3 and 4.

Referring now to FIGURE 7, there is illustrated a flow diagram of the method for obtaining a digital signature utilizing a crypto module 70. The document 10 to be signed is received at step 80 and displayed
30 by the crypto module 70 using the browser 65 at step 85. The mobile terminal 20 authenticates the PC 60 and crypto module 70 at step 90 and

establishes a communications channel 75 at step 95. The hash 15 of the document 10 is transmitted at step 100 to the mobile terminal 20 such that the hash 15 may be displayed at step 105 on a display of the mobile terminal 20. The user views the displayed hash 15 at the mobile terminal and the document 10 displayed at the crypto module 70 and provides at step 110 a digital signature of the document 10.

Referring now to FIGURE 8, there is illustrated a further embodiment for obtaining a digital signature of a document 10 wherein a trusted party 115 is used. In this embodiment, after receipt of a document 10, a PC 120 forwards the document through a web server 125 to the trusted party 115. Within the web server 125 a servlet 130 generates a hash 15 that is to be signed by the user at the mobile terminal 20. The hash 15 and document 10 are forwarded from the web server 125 to the trusted party 115, and the hash is forwarded to the mobile terminal 20 via a communications channel 135. The data is transmitted from the PC 120 to the web server 125 and from the web server 125 to the trusted party 115 using SSL/TLS protocol.

Referring now to FIGURE 9, there is provided a flow diagram more fully illustrating a method for obtaining a digital signature using a personal trusted device such as a mobile terminal 20 through a trusted party 115. The document 10 to be signed is received at the PC 120 at step 140, and a user requests a digital signature at the PC 120 at step 145. The trusted party 115 authenticates the PC 120 at step 150 before the connection established from the PC 120 to the web server 125 to the trusted party 115. Alternatively, the PC 120 may have been previously securely identified at the trusted party 115 and already have a registered mobile terminal 20 on file with the trusted party 115 for the transaction.

After the PC 120 has been authenticated, the request for a digital signature is transmitted to the web server 125 at step 155 along with the document 10. The servlet 130 generates a hash 15 from the provided

document 10. The hash 15 along with the document 10 and the request for the digital signature are forwarded at step 165 to the trusted party 115 from the web server 125. The trusted party 115 sends at step 170 the hash 15 to the mobile terminal 20 over a communications channel 135.

5 After viewing the document at the trusted third party, the mobile terminal provides the digital signature at step 180, and the mobile terminal 20 notifies the trusted party 115 of the signature at step 185. The trusted party validates the provided digital signature and updates and notifies the transaction as being signed at both the PC 120 and

10 mobile terminal 20 at step 190.

Referring now to FIGURE 10, there is illustrated yet another embodiment wherein a PC 200 transmits a document 10 to the mobile terminal 20 as streaming data. The general concept behind the use of streaming data is that all or a large portion of the data, not only the

15 hash, shall be transmitted to the mobile terminal 20 for signature generation. The data to be signed is displayed at the PC 200 and is streamed to the mobile terminal 20. The problem still exists that the entire document cannot be displayed to a user on a small screen of the mobile terminal 20, and the internal buffers of the mobile terminal 20

20 are not normally large enough to store a large document. This requires the use of one of two solutions described in more detail in FIGURES 11 and 12.

Referring now to FIGURE 11, there is illustrated a method wherein a user utilizes a mouse at the PC 200 to select relevant text at step

25 205 that the user considers to be essential. The selected text and the hash 15 are transmitted to the mobile terminal at step 210. The user digitally signs the received information at step 215 after viewing the provided text and the hash 15.

Referring now to FIGURE 12, there is illustrated an alternative embodiment wherein a user may trigger a button or activation point at

30 step 220 of the mobile terminal 20. Responsive to the trigger, the

mobile terminal 20 displays the present content of its buffers at step 225. The user may then digitally sign a document at step 230 based upon what is viewed.

5 Despite being unable to display or even store a large document 10, the mobile terminal 20 may be able to receive the text of the document 10 from the PC and compute the hash 15 from the received text. The hash 15 computed in the mobile terminal 20 can then be compared in the mobile terminal 20 with the hash 15 transmitted by the PC which the user is being invited to sign. Other checks such as byte count can also be
10 computed in the mobile terminal 20 to verify that the document 10 to which the hash code 15 applies is the claimed document 10. It would be preferable to include the document byte count as part of the bytestring over which the hash code 15 is computed. The above steps provide additional security safeguards to the user that he is signing what he
15 thinks he is signing.

Referring now to FIGURE 13, there is illustrated an alternative embodiment for providing a digital signature including a customer PC 250, a merchant server 255 and a customer mobile electronic transaction (MeT) device 260. The customer PC 250 includes a web browser 265
20 enabling the user to access the merchant server 255 via a network such as the Internet. The customer PC 250 further includes a mobile electronic terminal personal proxy (MPP) 270 for controlling electronic commerce transactions between the customer PC 250, the merchant server 255 and the customer Mobile electronic transaction device 260. The MPP
25 270 is accessed via the web browser 265. The MPP 270 comprises a software module that is executable by the customer PC 250. Communications between the browser 265 and MPP 270 and between the MPP 270 and the merchant server 255 use HTTP protocol (extended to handle the Mobile electronic transaction specific header information) over
30 TCP/IP. The MPP 270 enables the customer PC 250 to act as a server for a Mobile electronic transaction device 260. Access to the Mobile

electronic transaction device 260 will only require user provided authentication (password, PIN) when payment is requested.

An application 275 within the customer PC provides any of a number of functionalities with respect to an electronic commerce transaction.

5 With respect to the following description of the method of the present invention, the application 275 will provide a digital signature functionality wherein a data string provided from the merchant server 255 may have a digital signal appended thereto by the application 275.

The web server 280 provides the ability for the mobile terminal to

10 connect to services in the PC 250. The WAP gateway 285 provides for the ability of a wireless device such as the Mobile electronic transaction device 260 to access the Internet using the WAP protocol through the customer PC 250. The WAP gateway 285 acts as an interface between a WAP network and a TCP/IP network such as the Internet. The WAP gateway 285

15 converts between the WAP and TCP/IP protocols.

The Bluetooth stack 290 enables the customer PC 250 to generate a short range wireless link with the Mobile electronic transaction device 260 within a limited, defined area using the Bluetooth protocol. While the present invention is described with the use of a short range

20 wireless link using the Bluetooth protocol, it should be realized that any other short range wireless protocol enabling the customer PC 250 to access a closely located Mobile electronic transaction device 260 or other information devices would be useful within the context of the present invention.

25 The mobile electronic transaction device 260 may consist of a mobile telephone, laptop computer, personal data assistant, or any other similarly configured mobile electronic device which contains information necessary to complete an electronic commerce transaction. The merchant server 255 includes applications 295 for performing necessary

30 functionalities for completing an electronic commerce transaction with the customer PC 250 and a web server 300 enabling the merchant server to

obtain access to a network such as the Internet.

Referring now also to FIGURE 14, there is illustrated a flow diagram illustrating the manner in which the MPP 270 controls a request for performance of a digital signature between a customer PC 250, merchant server 255 and Mobile electronic transaction device 260. At step 305, a request is transmitted from the web browser 265 to the MPP 270. The MPP 270 forwards the request to the web server 300 of the merchant server 255 at step 310. The request may comprise a request to purchase a particular item or to download already purchased products.

In order to process the request, the merchant server 255 requires a digital signature from the customer. The merchant server 255 responds to the request by transmitting at step 315 a response that includes a specific data string and a request for digital signature to be attached to the data string. The merchant response to the request from the MPP 270 comprises a URI containing a specific HTTP 1.1 header: for example: [Mobile electronic transaction-sign: "http://merchantsite.com/responsesite/", "String to sign"]. This comprises an instruction for the Mobile electronic transaction device 260 to sign the attached data string and transmit the digitally signed data string back to the indicated HTTP site. The MPP 270 will pass most requests or responses through without taking action. However, once a Mobile electronic transaction command is detected within a request or response the MPP 270 is actuated. The MPP 270 recognizes the Mobile electronic transaction command included in the HTTP header and transmits at step 320 a notification to the browser 265 indicating a digital signature has been requested. It should be realized that Mobile electronic transaction commands other than a request for a digital signal may also be utilized. The web browser 265 will display a page having a PRAGMA REFRESH (fetch from server when reloaded, i.e., do not cache) header command while the digital signature is obtained.

The data string within the response from the merchant server 255

is forwarded at step 325 to the application 275 within the customer's PC 250. Responsive to the received data string, the application 275 transmits at step 330 a command to the Bluetooth stack 290. The command instructs the Bluetooth stack 290 to awaken the Mobile electronic transaction device 260, if possible. The awakening is accomplished by transmitting an AT command to the Mobile electronic transaction device 260 using Bluetooth at step 335. Responsive to this awakening, the Mobile electronic transaction device 260 will request at step 336 the same application of the Mobile electronic transaction device 260. The application within the Mobile electronic transaction device 260 executes at step 340 a WML script code that will provide a request containing the digital signature (response). At step 345 the response including the digital signature is transmitted to the web server 280 via the Bluetooth stack 290 and WAP Gateway 285. The response is then passed to the application 275. The application 275 appends the digital signature to the provided data string at step 350 and notifies the Bluetooth stack 290 of the completed signature at step 355.

The application 275 forwards at step 360 the digitally signed data string back to the MPP 270. The MPP 270 notifies the browser at step 365 of the completed signing of the data string which then begins reloading a URI displaying an indication that the data string has been signed. The MPP transmits at step 370 an HTTP request to the URL contained in the original HTTP header (<http://merchantsite.com/responsesite/>) containing the signed data string. Upon receipt of the signed data string the web server 300 within the merchant server 255 transmits a response back to the MPP at 375 notifying the web browser 265 of the customer PC that the transaction is completed.

It should be emphasized that the term "comprises/comprising" when used in this specification is taken to specify the presence of stated features, integers, steps or components but does not preclude the

presence or addition of one or more features, integers, steps, components or groups thereof.

The previous description is of a preferred embodiment for implementing the invention, and the scope of the invention should not
5 necessarily be limited by this description. The scope of the present invention is instead defined by the following claims.

WHAT IS CLAIMED IS:

1. A method for digitally signing a document, comprising the steps of:
5 receiving the document to be digitally signed at a first location;
generating a representation of the document;
forwarding the representation of the document to a personal trusted device; and
10 digitally signing the representation of the document at the personal trusted device.
2. The method of Claim 1, wherein the first location comprises a trusted PC.
15
3. The method of Claim 2, further including the step authenticating an identity of the trusted PC by the personal trusted device.
- 20 4. The method of Claim 2, wherein the step of digitally signing further includes the step of entering a PIN into the personal trusted device.
- 25 5. The method of Claim 2, wherein the step of forwarding further comprises the steps of establishing a serial cable connection between the personal trusted device and the trusted PC.
- 30 6. The method of Claim 2, wherein the step of forwarding further comprises the steps of establishing a infrared connection between the personal trusted device and the trusted PC.

7. The method of Claim 2, wherein the step of forwarding further comprises the steps of establishing a Bluetooth connection between the personal trusted device and the trusted PC.

5 8. The method of Claim 2, further including the step of displaying the document at the trusted PC prior to digitally signing the representation.

9. The method of Claim 1, wherein the first location comprises
10 a cryptography module within a PC.

10. The method of Claim 9, further including the step of displaying the document at the PC in a browser associated with the cryptography module.

15 11. The method of Claim 1, further including the step of forwarding the document from the first location to a trusted third party.

20 12. The method of Claim 11, wherein the step of forwarding further comprises forwarding the documents from the first location to the trusted third party using SSL/TLS.

25 13. The method of Claim 1, wherein the step of forwarding further comprises the steps of:

forwarding the document to a server prior to generation of the representation of the document;

forwarding the document and the representation of the document from the server to the trusted party.

14. The method of Claim 1, wherein the step of forwarding the representation further comprises the step of streaming the representation and at least a portion of the document to the personal
5 trusted device.

15. The method of Claim 14, further including the step of:
selecting portions of the document to be streamed to the personal
trusted device; and
10 displaying the selected portions at the personal trusted device.

16. The method of Claim 14, further including the step of
displaying only portions of the document contained within a buffer of the
personal trusted device.
15

17. The method of Claim 1, further comprising the steps of:
forwarding the document to the personal trusted device;
generating a second representation of the document at the
personal trusted device; and
20 comparing the representation with the second representation
of the document.

18. The method of Claim 1, wherein the document comprises an
email.
25

19. A method for digitally signing a document, comprising the
steps of:
receiving the document to be digitally signed at a personal
computer;
30 generating a hash from the document at the personal
computer;

authenticating the personal computer from a mobile terminal;
forwarding the hash to the mobile terminal; and
displaying the document at the personal computer;
displaying the hash at the mobile terminal; and
5 digitally signing the hash of the document at the mobile
terminal.

20. The method of Claim 19, wherein the step of digitally
signing further includes the step of entering a PIN into the mobile
10 terminal.

21. The method of Claim 19, wherein the step of forwarding
further comprises the steps of establishing a serial cable connection
between the mobile terminal and the personal computer.
15

22. The method of Claim 19, wherein the step of forwarding
further comprises the steps of establishing an infrared connection
between the mobile terminal and the personal computer.

20 23. The method of Claim 19, wherein the step of forwarding
further comprises the steps of establishing a Bluetooth connection
between the mobile terminal and the personal computer.

24. The method of Claim 19, wherein the step of displaying the
25 document at the personal computer further comprises the step of
displaying the document in a browser at the personal computer.

25. The method of Claim 19, wherein the personal computer
comprises a trusted personal computer.
30

26. The method of Claim 19, wherein the step of generating comprises the step of generating the hash from the document at a cryptography module in the personal computer.

5 27. The method of Claim 19, further comprising the steps of:
 forwarding the document to the personal trusted device;
 generating a second hash of the document at the personal
 trusted device; and
 comparing the hash with the second representation of the
10 document.

28. The method of Claim 19, wherein the document comprises an email.

15 29. A method for digitally signing a document, comprising the steps of:
 receiving the document to be digitally signed at a personal
 computer;
 forwarding the document to a server;
20 generating a hash from the document at the server;
 forwarding the hash and the document from the server to a
 trusted third party from the server;
 forwarding the hash to a mobile terminal from the trusted
 third party; and
25 digitally signing the hash of the document at the mobile
 terminal.

30 30. The method of Claim 29, wherein the steps of forwarding further comprises forwarding the documents using SSL/TLS protocol.

31. The method of Claim 29, further including the step of

requesting a digital signature at the PC.

32. A method for digitally signing a document, comprising the steps of:

- 5 receiving the document to be digitally signed at a personal computer;
- generating a hash from the document at the personal computer;
- streaming the hash and at least a portion of the document to
- 10 a mobile terminal; and
- digitally signing the hash at the mobile terminal.

33. The method of Claim 32, further including the step of:

- selecting portions of the document to be streamed to the mobile
- 15 terminal.

34. The method of Claim 32, further including the step of displaying only portions of the document contained within a buffer of the mobile terminal.

20

35. A system for digitally signing a document, comprising the steps of:

- a personal computer for receiving the document to be digitally signed and enabling generation of a hash of the document; and
- 25 a personal trusted device for displaying the hash and for enabling digital signing of the hash.

36. The system of Claim 35, wherein the personal computer further displays the document.

30

37. The system of Claim 35, wherein the personal computer

further includes a cryptographic module for enabling generation of the hash.

38. The system of Claim 35, further including:
5 a server for generating the hash from the document; and
a trusted party for providing the hash to the personal
trusted device.

39. The system of Claim 35, wherein the personal computer
10 streams the hash and at least a portion of the document to the mobile
terminal.

40. The system of Claim 35, wherein the document comprises an
email.

1/5

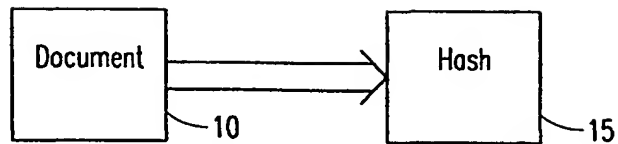


FIG. 1

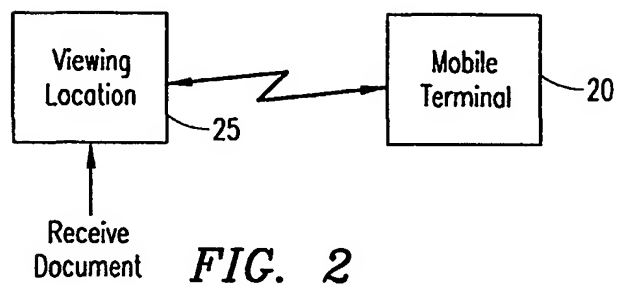


FIG. 2

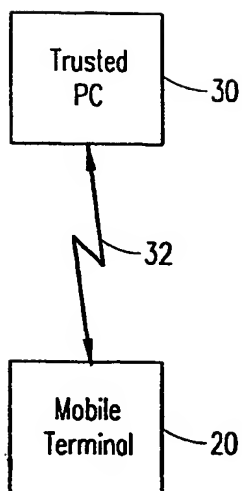


FIG. 3

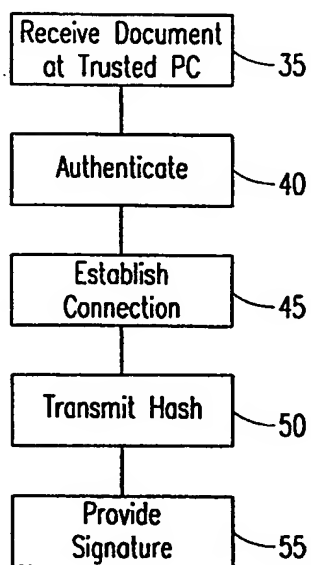


FIG. 4

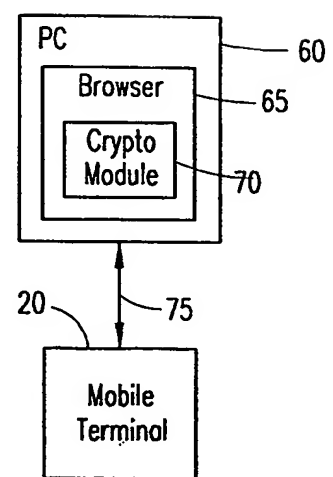


FIG. 5

2/5

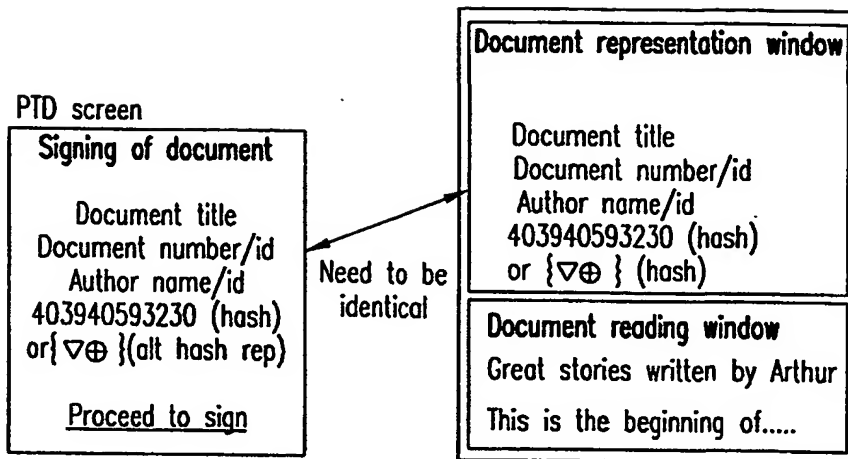


FIG. 6

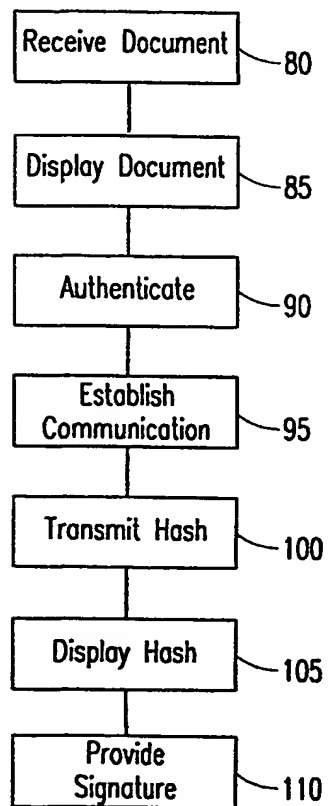


FIG. 7

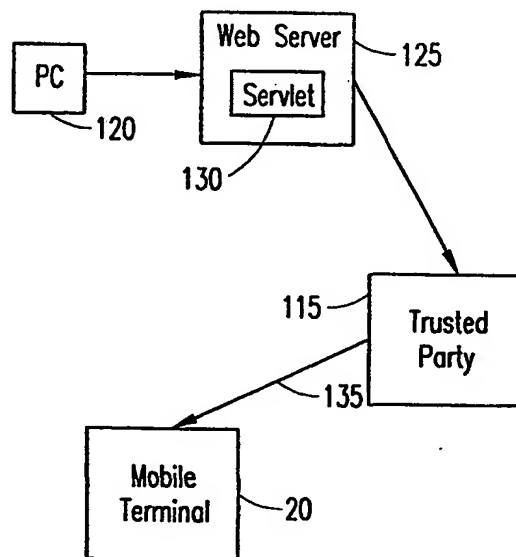
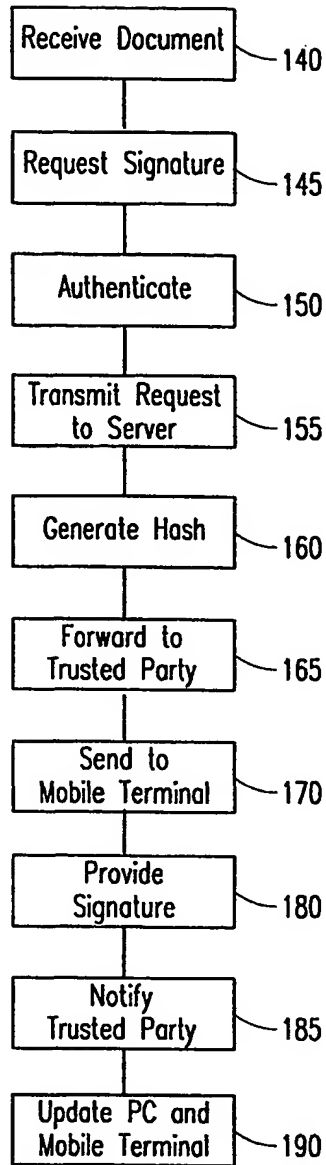
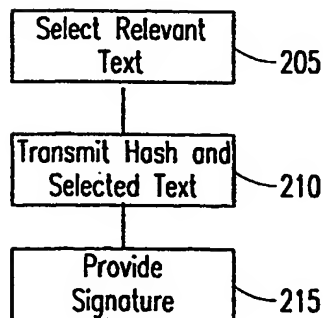
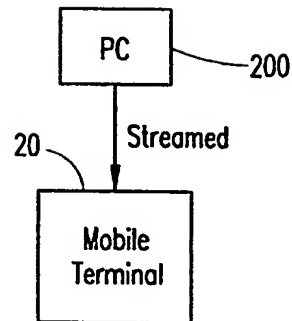
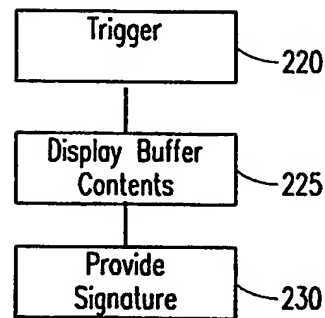


FIG. 8

**FIG. 9****FIG. 11****FIG. 10****FIG. 12**

4/5

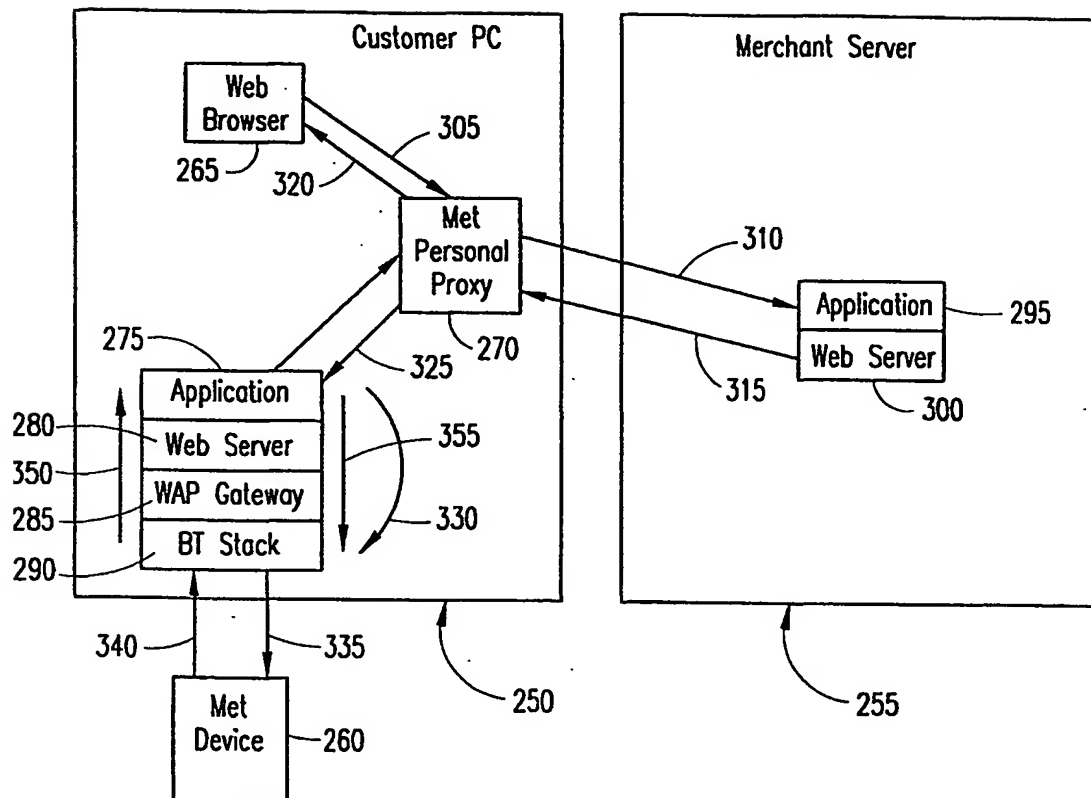


FIG. 13

5/5

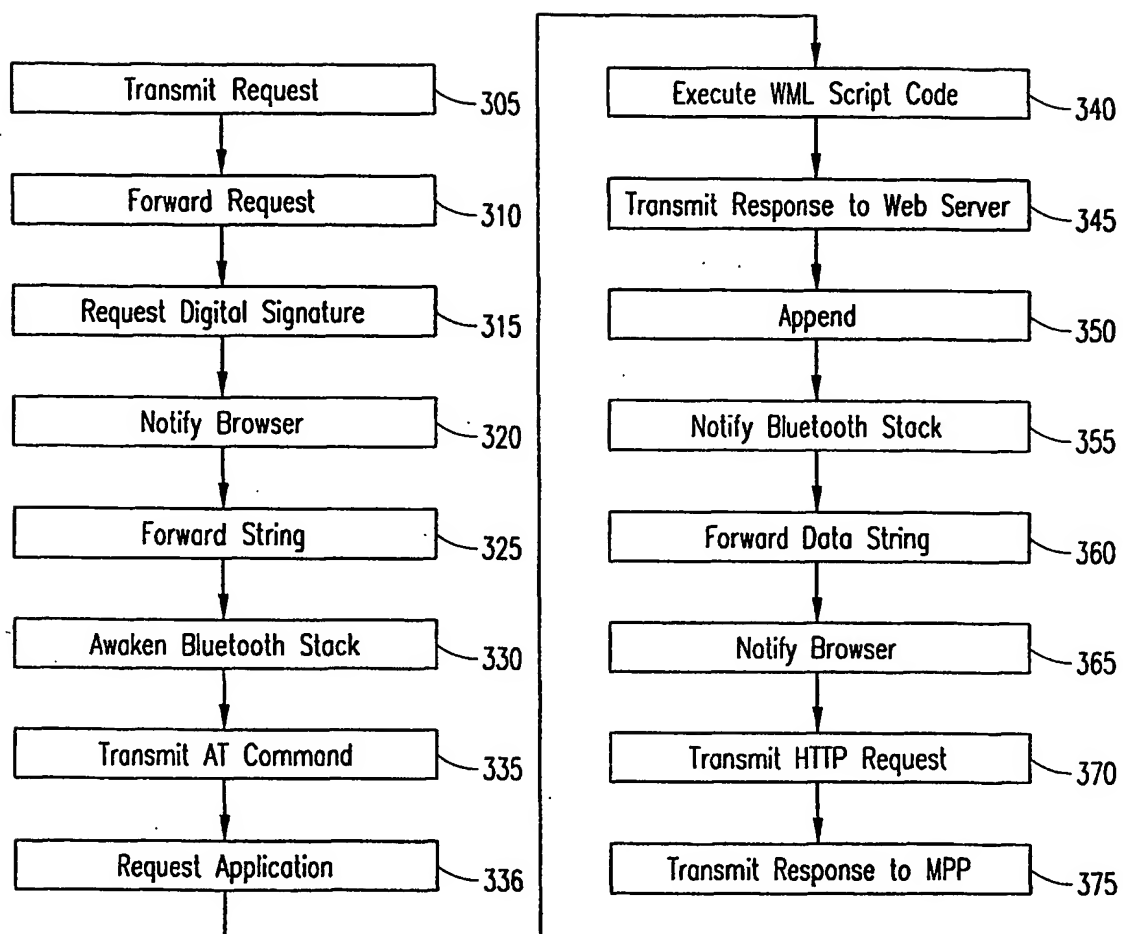


FIG. 14

THIS PAGE BLANK (USPTO)